

Sicherheitshandbuch zu Oracle Hardware Management Pack

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. AMD, Opteron, das AMD-Logo und das AMD Opteron-Logo sind Marken oder eingetragene Marken der Advanced Micro Devices. UNIX ist eine eingetragene Marke der The Open Group.

Diese Software oder Hardware und die zugehörige Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Inhalt

Überblick	5
Produktüberblick	5
Info zu diesem Sicherheitshandbuch	6
Sicherheitsgrundsätze	6
Sicherheitsübersicht zu Oracle Hardware Management Pack	7
Oracle Hardware Management Pack - Vor der Installation	9
Komponenten von Oracle Hardware Management Pack	9
Sicherheitseinstellungen von SNMP-Plug-in basierend auf Agent	10
Wählen einer SNMP-Protokollversion für den SNMP-Agent	10
Oracle Hardware Management Pack - Installation	11
Ausführen des Installationsprogramms für Oracle Hardware Management Pack	11
Aktivieren von LAN-Interconnect	11
Speichern von Zugangsdaten in einer Datei	12
Oracle Hardware Management Pack - Nach der Installation	15
Deinstallation von Oracle Hardware Management Pack	15

Überblick

Dieser Abschnitt enthält einen Überblick über Oracle Hardware Management Pack-(HMP-)Produkt, einschließlich Sicherheitshandbuchinformationen. Außerdem werden die allgemeinen Grundlagen der Anwendungssicherheit erläutert.

Folgende Themen werden behandelt:

- „Produktüberblick“ auf Seite 5
- „Info zu diesem Sicherheitshandbuch“ auf Seite 6
- „Sicherheitsgrundsätze“ auf Seite 6
- „Sicherheitsübersicht zu Oracle Hardware Management Pack“ auf Seite 7

Produktüberblick

Oracle Hardware Management Pack ist für Ihren Server, zahlreiche andere x86-basierte Server sowie für einige SPARC-basierte Server verfügbar. Oracle Hardware Management Pack besteht aus zwei Komponenten: einem SNMP-Überwachungsagent sowie einer Familie von betriebssystemübergreifenden CLI-Tools (Command-Line Interface) für die Serververwaltung.

In Verbindung mit den SNMP-Plug-ins von Hardware Management Agent können Sie SNMP zur Überwachung von Oracle-Servern und -Servermodulen in Ihrem Rechenzentrum einsetzen, ohne dass Sie sich mit zwei Verwaltungspunkten (Host und Oracle ILOM) verbinden müssen. Durch diese Funktion kann eine einzelne IP-Adresse (IP des Hosts) zur Überwachung von mehreren Servern und Servermodulen verwendet werden.

Hardware Management Agent-SNMP-Plug-ins werden auf dem Hostbetriebssystem von Oracle-Servern ausgeführt. Die SNMP-Plug-ins kommunizieren über die Oracle Hardware Storage Access Librarys mit dem Serviceprozessor. Informationen zum aktuellen Status des Servers werden automatisch vom Hardware Management Agent abgerufen.

Zur Konfiguration von Oracle-Servern können Sie Oracle Server CLI Tools verwenden. Die CLI-Tools sind kompatibel mit Oracle Solaris, Oracle Linux, Oracle VM, weiteren Linux-Distributionen und Windows-Betriebssystemen. In der folgenden Tabelle werden die Aufgaben beschrieben, die Sie mit den CLI-Tools ausführen können.

Systemverwaltungsaufgabe von Host-BS	CLI-Tool
BIOS-Einstellungen, Bootreihenfolge der Geräte und einige Serviceprozessoreinstellungen konfigurieren.	ubiosconfig biosconfig
Oracle ILOM und BIOS aktualisieren.	fwupdate
Firmware-Versionen auf unterstützten SAS-Speichergeräten, eingebetteten SAS-Speicher-Controllern, SAS-Speichererweiterungen und Speicherlaufwerken abfragen, aktualisieren und validieren.	
Oracle ILOM-Konfigurationseinstellungen wiederherstellen, festlegen und anzeigen sowie Oracle ILOM-Eigenschaften anzeigen und festlegen, die mit der Netzwerkverwaltung, Uhrenkonfiguration und Benutzerverwaltung verbunden sind.	ilomconfig
RAID-Datenträger auf Speicherlaufwerken, die mit RAID-Controllern verbunden sind, einschließlich Speicherarrays anzeigen oder erstellen.	raidconfig
Systemintegrität überwachen.	hwmgmt

Info zu diesem Sicherheitshandbuch

Dieses Dokument enthält allgemeine Sicherheitsrichtlinien für Oracle Hardware Management Pack. Dieses Handbuch soll Ihnen dabei helfen, die Sicherheit zu gewähren, wenn Sie die Software mit anderen Oracle-Hardwareprodukten, wie Netzwerk-Switches und Netzwerkkarten, verwenden.

Folgende Themen werden behandelt:

- „Überblick“ auf Seite 5
- „Oracle Hardware Management Pack - Vor der Installation“ auf Seite 9
- „Oracle Hardware Management Pack - Installation“ auf Seite 11
- „Oracle Hardware Management Pack - Nach der Installation“ auf Seite 15

Sicherheitsgrundsätze

Zu den Sicherheitsgrundsätzen zählen Zugang, Authentifizierung, Autorisierung und Überwachung.

- Zugang
 - Schützen Sie Ihre Hardware und Ihre Daten durch physische und virtuelle Steuerungsmechanismen vor unerlaubten Zugriffen.
 - Bei der Hardware bedeutet dies normalerweise physische Zugriffsbeschränkungen.
 - Bei Software sollten Sie sowohl den physischen als auch den virtuellen Zugang beschränken.
 - Firmware kann ausschließlich durch den Updateprozess von Oracle geändert werden.

- Authentifizierung

Richten Sie alle Funktionen zur Authentifizierung ein, wie ein Kennwortsystem in den Betriebssystemen Ihrer Plattform, sodass festgestellt werden kann, ob es sich bei einem Benutzer wirklich um diesen Benutzer handelt.

Die Authentifizierung bietet unterschiedliche Sicherheitsgrade über Maßnahmen wie Ausweise und Kennwörter. Beispiel: Stellen Sie sicher, dass das Personal beim Betreten eines Computerraums Mitarbeiterausweise trägt.

- Autorisierung

Durch die Autorisierung können Mitarbeiter nur mit der Hardware und Software arbeiten, für die sie geschult wurden.

Beispiel: Legen Sie Berechtigungen für das Lesen, Schreiben und Ausführen fest, um den Zugriff von Benutzern auf Befehle, Festplattenspeicher, Geräte und Anwendungen zu kontrollieren.

- Überwachung

Kunden-IT-Mitarbeiter können Software- und Hardwarefunktionen von Oracle zur Überwachung von Anmeldevorgängen und zur Wartung der Hardware verwenden.

- Überwachen Sie die Anmeldung von Benutzern anhand von Systemlogs. Verfolgen Sie insbesondere Systemadministrator- und Serviceaccounts über Systemlogs, da vor allem diese Accounts Zugriff auf leistungsstarke Befehle gewähren.
- Stufen Sie Logdateien regelmäßig als veraltet ein, wenn diese gemäß der Unternehmensrichtlinie des Kunden eine bestimmte Größe überschreiten. Logs werden normalerweise für einen langen Zeitraum beibehalten und müssen daher unbedingt gepflegt werden.
- Verfolgen Sie Systemressourcen für Bestandszwecke anhand von Komponentenseriennummern. Oracle-Teilenummern sind auf allen Karten, Modulen und Hauptplatinen elektronisch gespeichert.

Sicherheitsübersicht zu Oracle Hardware Management Pack

Die folgenden wichtigen Sicherheitspunkte müssen bei der Konfiguration aller Systemverwaltungstools berücksichtigt werden:

- *Systemverwaltungsprodukte können dazu verwendet werden, eine bootfähige Root-Umgebung zu erhalten.*

Mittels einer bootfähigen Root-Umgebung können Sie Zugriff zu Oracle ILOM, Oracle System Assistant und zu Festplatten erhalten.

- *Systemverwaltungsprodukte enthalten leistungsstarke Tools, für deren Ausführung Administrator- oder Root-Berechtigungen erforderlich sind.*

Mit dieser Berechtigungsstufe ist es möglich, die Hardwarekonfiguration zu ändern und Daten zu löschen.

- Dokumentations-Library für Oracle Hardware Management Pack (<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Oracle Hardware Management Pack - Vor der Installation

Verwenden Sie bei der Erstinstallation und -konfiguration Oracle-Softwaresicherheitsfunktionen, um die Hardware zu steuern und Systemressourcen zu verfolgen.

Folgende Themen werden behandelt:

- „Komponenten von Oracle Hardware Management Pack“ auf Seite 9
- „Sicherheitseinstellungen von SNMP-Plug-in basierend auf Agent“ auf Seite 10
- „Wählen einer SNMP-Protokollversion für den SNMP-Agent“ auf Seite 10

Komponenten von Oracle Hardware Management Pack

Oracle Hardware Management Pack umfasst eine Sammlung aus Befehlszeilentools für die Hardwareverwaltung zur Konfiguration von RAID, BIOS und Oracle ILOM und zur Aktualisierung der Firmware. Es enthält außerdem ein SNMP-Plug-in zur Überwachung. Oracle Hardware Management Pack enthält darüber hinaus einen Daemon oder Service, der über einen internen Kanal mit Oracle ILOM kommuniziert, um Bestands- und Integritätsinformationen zum Server weiterzugeben.

Diese Tools und Plug-ins werden auf dem Hostbetriebssystem installiert, sodass Sie Systemverwaltungsaufgaben direkt vom Host ausführen können. Oracle Hardware Management Pack enthält zwar nützliche Funktionen für die Verwaltung eines Oracle-Servers, ist aber optional.

Weitere Informationen zu den Funktionen von Oracle Hardware Management Pack finden Sie im Sun Server Hardware Management Pack User's Guide, um zu bestimmen, ob Sie diese verwenden und installieren möchten.

- Dokumentations-Bibliothek für Oracle Hardware Management Pack (<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)
- Allgemeine Oracle ILOM-Informationen finden Sie unter: <http://www.oracle.com/pls/topic/lookup?ctx=ilom31>

Sicherheitseinstellungen von SNMP-Plug-in basierend auf Agent

Oracle Hardware Management Pack umfasst ein SNMP-Plug-in-Modul, mit dem der native SNMP-Agent im Hostbetriebssystem um zusätzliche Oracle MIB-Funktionen erweitert wird. Es muss besonders darauf hingewiesen werden, dass Oracle Hardware Management Pack selbst keinen SNMP-Agent enthält. Bei Linux wird dem net-snmp-Agent, der zunächst installiert werden muss, ein Modul hinzugefügt. Bei Solaris wird dem Solaris Management Agent ein Modul hinzugefügt. Bei Windows wird der native SNMP-Service durch das Plug-in erweitert.

So werden alle SNMP-bezogenen Sicherheitseinstellungen für das Oracle Hardware Management Pack-SNMP-Plug-in durch die Einstellungen des nativen SNMP-Agents oder Service und nicht durch das Plug-in bestimmt. Anweisungen zum sicheren Konfigurieren von SNMP finden Sie in der Dokumentation für net-snmp oder für den Windows-SNMP-Service.

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/pls/topic/lookup?ctx=ohmp\)](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)

Wählen einer SNMP-Protokollversion für den SNMP-Agent

SNMP ist ein Standardprotokoll, das zur Systemüberwachung oder -verwaltung verwendet wird. SNMPv1/v2c bietet keine Verschlüsselung und führt die Authentifizierung anhand von Communityzeichenfolgen durch. Communityzeichenfolgen werden über das Netzwerk in Klartext übertragen und üblicherweise von einer Gruppe gemeinsam und nicht von einem einzelnen Benutzer privat genutzt. Bei SNMPv3 hingegen wird durch die Verschlüsselung ein sicherer Kanal bereitgestellt, und es werden Benutzernamen und Kennwörter verwendet. SNMPv3-Benutzerkennwörter sind lokalisiert, sodass sie sicher auf Verwaltungsstationen gespeichert werden können.

Oracle empfiehlt die Verwendung von SNMPv3, wenn dies vom nativen SNMP-Agent unterstützt wird. Anweisungen zum Konfigurieren von SNMPv3 finden Sie in der Dokumentation für net-snmp oder für den Windows-SNMP-Service.

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/pls/topic/lookup?ctx=ohmp\)](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)

Oracle Hardware Management Pack - Installation

Folgende Themen werden behandelt:

- „Ausführen des Installationsprogramms für Oracle Hardware Management Pack“ auf Seite 11
- „Aktivieren von LAN-Interconnect“ auf Seite 11
- „Speichern von Zugangsdaten in einer Datei“ auf Seite 12

Ausführen des Installationsprogramms für Oracle Hardware Management Pack

Oracle Hardware Management Pack besteht aus einer Reihe von nativen Installationspackages, die mit den nativen Installationstools für ein Betriebssystem, wie RPM, installiert werden können. Darüber hinaus kann ein assistentenbasiertes Installationsprogramm bei der Installation behilflich sein. Mit dem Installationsprogramm werden die nativen Packages hinzugefügt und die Verwendung von Oracle Hardware Management Pack konfiguriert.

Da das Installationsprogramm für Oracle Hardware Management Pack native Packages installieren muss, müssen Sie es als Root oder Administrator ausführen.

- [Dokumentations-Library für Oracle Hardware Management Pack \(http://www.oracle.com/pls/topic/lookup?ctx=ohmp\)](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)

Aktivieren von LAN-Interconnect

Eine schnellere Alternative zur KCS-Schnittstelle ist die interne High-Speed Interconnect-Verbindung, über die Clients auf dem Hostbetriebssystem mit Oracle ILOM kommunizieren können. Dieses Interconnect wird durch eine interne Ethernet-USB-Verbindung implementiert, und es wird ein IP-Stack ausgeführt. Oracle ILOM und der Host erhalten interne, nicht weiterleitbare IP-Adressen für die Kommunikation über diesen Kanal.

Für die Verbindung mit Oracle ILOM über das LAN-Interconnect ist, genau wie für eine Netzwerkverbindung mit dem Oracle ILOM-Verwaltungsport, eine Authentifizierung erforderlich. Alle im Verwaltungsnetzwerk bekannten Services und Protokolle stehen dem

Host über das LAN-Interconnect zur Verfügung. Beispiel: Sie können die Oracle ILOM-Webbenutzeroberfläche aufrufen, indem Sie einen Webbrowser auf dem Host verwenden oder mithilfe eines Secure Shell-Clients eine Verbindung mit der Oracle ILOM-Befehlszeilenschnittstelle aufbauen. In allen Fällen ist ein gültiger Benutzername und ein gültiges Kennwort für das LAN-Interconnect erforderlich.

Das Installationsprogramm für Oracle Hardware Management Pack enthält eine Option zum Aktivieren des LAN-Interconnects. Oracle empfiehlt die Aktivierung des LAN-Interconnects nur, wenn die Netzwerkanweisung RFC 3927 sowie die Fähigkeit für Link-Local-IPv4-Adressen unterstützt. Sie sollten außerdem sicherstellen, dass das Betriebssystem nicht als Bridge oder Router verwendet wird. Dadurch wird sichergestellt, dass der Verkehrsverkehr zwischen dem Host und Oracle ILOM privat bleibt.

- **Dokumentations-Library für Oracle Hardware Management Pack** (<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Speichern von Zugangsdaten in einer Datei

Die Tools "ilomconfig" und "fwupdate", die Teil von Oracle Hardware Management Pack sind, können über das High-Speed-LAN-Interconnect eine Verbindung zu Oracle ILOM herstellen. Durch die Verwendung des LAN-Interconnects anstelle der langsameren KCS-Schnittstelle kann die Performance von wesentlichen Vorgängen, wie Oracle ILOM-Firmware-Updates, erheblich verbessert werden.

Da für das LAN-Interconnect die Authentifizierung erforderlich ist, müssen Sie sich bei jedem Aufruf dieser Tools bei Oracle ILOM authentifizieren. Um dies zu erleichtern, können Sie die Zugangsdaten in einer Datei cachen, damit sie automatisch von den Tools verwendet werden können. So müssen Sie keine Klartext-Kennwörter in Skripte einbetten, die die Oracle Hardware Management Pack-Tools verwenden.

Mit dem Tool "ilomconfig" können Sie den Benutzernamen und das Kennwort in einer verschlüsselten Datei speichern, die auf Root-Ebene schreibgeschützt ist. Wenn Sie mit ilomconfig oder fwupdate auf Oracle ILOM zugreifen und diese Datei ermittelt wird, werden die gecachten Zugangsdaten verwendet. Alternativ dazu können Sie den Benutzernamen und das Kennwort bei jedem Aufruf des Tools in der Befehlszeile angeben.

Der verwendete Verschlüsselungsalgorithmus ist in jedem System eindeutig. Wenn der Schlüssel ermittelt wird, könnte die Datei allerdings entschlüsselt werden und den Benutzernamen und das Kennwort freigeben. Oracle empfiehlt daher die Erstellung eines eindeutigen Kennworts in jedem Oracle ILOM, sodass ein freigegebenes Kennwort nicht für andere Oracle ILOM-Systeme verwendet werden kann.

Anweisungen zum Speichern der Zugangsdaten in einer Datei finden Sie im Sun Server Hardware Management Pack User's Guide.

- Dokumentations-Library für Oracle Hardware Management Pack (<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Oracle Hardware Management Pack - Nach der Installation

Folgende Themen werden behandelt:

- „Deinstallation von Oracle Hardware Management Pack“ auf Seite 15

Deinstallation von Oracle Hardware Management Pack

Die Oracle Hardware Management Pack-Packages können mit nativen Packagetools, wie RPM, oder mit dem assistentenbasierten Deinstallationsprogramm aus dem Lieferumfang von Oracle Hardware Management Pack deinstalliert werden. Wenn Packages mit nativen Packages entfernt werden, wird die verschlüsselte Datei mit dem gecachten Benutzernamen und Kennwort für das LAN-Interconnect nicht gelöscht. Sie muss manuell gelöscht werden.

Beim assistentenbasierten Deinstallationsprogramm wird die Zugangsdatendatei entfernt. Daher wird empfohlen, Oracle Hardware Management Pack mit dem assistentenbasierten Installationsprogramm zu deinstallieren.

- Dokumentations-Library für Oracle Hardware Management Pack (<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

